State of West Virginia Office of Technology
Policy: Data Classification
Issued by the CTO

Policy No:	Issued:	Effective:	Revised:	Page 1 of 12
WVOT-PO100	01.06.10	04.06.10		

1.0 PURPOSE

This policy, issued by the West Virginia Office of Technology (WVOT), presents a framework through which all State of West Virginia (State) government agencies, employees, vendors, and business associates, specifically the Executive Branch, can classify data and systems as they relate to (1) data sensitivity; and (2) data and system criticality. (See Attachment A, *Data Sensitivity and System Criticality Grid*)

Consideration must be given to the fact that the same data type may have different sensitivity in different situations (e.g. publishing employee addresses: corrections employees vs. tourism employees).

2.0 SCOPE

This policy applies to all Executive Branch employees who have access to confidential and/or critical data and data systems.

3.0 RELEVANT DOCUMENTS/MATERIAL

3.1 West Virginia Code – "Duties of the Chief Technology Officer Relating to Security of Government Information" & "Categories of records to be preserved"

3.2 West Virginia Office of Technology (WVOT) Home Page

3.3 WVOT Policies Issued by the Chief Technology Officer (CTO)

3.4 Attachment A - Data Sensitivity and System Criticality Grid

3.5 WVOT-PO1001 – WVOT Information Security Policy

4.0 POLICY

4.1 Mandatory Data Classification

4.1.1 All State data requires classification, which is mandatory for more confidential and critical classes of data.

4.1.2 Data that is not classified will be reduced to a level of low sensitivity and criticality.

4.2 Certification and Management of Data

4.2.1 Each department and/or agency will provide annual certification that the data they collect, maintain, distribute, and ultimately destroy, is categorized in compliance with the data classification scheme prescribed in this policy.

4.2.2 Data must be properly managed according to its classification.

4.3 Training

4.3.1 All State employees with direct responsibility for State data (i.e. system owners, data owners, managers, and State leadership), must receive training in the data classification scheme appropriate to their role. (For example, State leadership must be trained and fully aware of the classification scheme of their departmental and agency employees who have a role in the maintenance of valid data classification, and of the implications of misclassified or non-classified data.)

4.3.1.1 Data owners must be trained and aware of the data classification scheme and the physical location of their sensitive and/or critical data and all secondary copies of that data.

4.3.1.2 Data owners must provide for the adequate synchronization of primary and secondary copies of this data, and must certify that the controls in place are commensurate with the sensitivity and criticality of the data. This includes access permissions and restrictions controls, as well as recovery strategies for lost or damaged data.

5.0 STANDARD PRACTICES

5.1 Data Classification Levels

Data owned and maintained by agencies will be put into appropriate classification levels, according to its sensitivity and criticality.

5.1.1 Level 1 – **Extremely Sensitive Data**

5.1.1.1 Extremely sensitive data is the most sensitive data to integrity and confidentiality risks. Disclosure or corruption of this data could be hazardous to life or health.

5.1.1.2 Access is tightly restricted with the most stringent security controls at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health, or safety repercussions. Individuals must adhere to very strict rules in the usage of this data.

5.1.1.3 Examples of extremely sensitive data may include the following:

5.1.1.3.1 Contents of State law enforcement investigative records; and

5.1.1.3.2 Child and adult protective services client data.

5.1.2 Level 2 – **Very Sensitive Data**

5.1.2.1 This data is only made available to authorized users and may be protected by federal and State regulations.

5.1.2.2 Access to very sensitive data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their job duties. These are the data elements removed

from responses to information requests for reasons of privacy.

5.1.2.3 Security threats to very sensitive data include violation of privacy statutes and regulations, as well as unauthorized alteration or destruction. If unauthorized persons accessed this data, it could cause financial loss or allow identity theft. In order to prevent these threats, security controls appropriate to the system containing this data must be in place.

5.1.2.4 Examples of very sensitive data may include the following:

5.1.2.4.1 Social Security numbers;

5.1.2.4.2 Credit card numbers;

5.1.2.4.3 Food assistance programs data;

5.1.2.4.4 Comprehensive law enforcement data;

5.1.2.4.5 Foster care data;

5.1.2.4.6 Health, mental health, acute medical care, and medical data;

5.1.2.4.7 Social Service or Temporary Assistance data; and

5.1.2.4.9 Tax information.

5.1.3 Level 3 – **Sensitive Data**

5.1.3.1 This data is made available through open record requests or other formal or legal processes; it includes the majority of the data contained within State government electronic databases.

5.1.3.2 Direct access is restricted to authenticated and authorized individuals who require access to that information in the course of performing their job duties.

5.1.3.3 Security threats to sensitive data include unauthorized access, alteration, and destruction concerns. Security controls appropriate to the system containing this data must be in place to prevent these threats.

5.1.3.4 Examples of sensitive data may include the following:

5.1.3.4.1 Most data elements in State personnel records;

5.1.3.4.2 Driver history records;

5.1.3.4.3 State/federal contracts data;

5.1.3.4.4 Employment and training program data;

5.1.3.4.5 Permits data; and

5.1.3.4.6 Historical records repository data.

5.1.4 Level 4 - **Unrestricted Data**

5.1.4.1 This data is characterized as being open, public data with no distribution limitations and to which anonymous access is allowed.

5.1.4.2 This type of information is: (1) actively made publicly available by State government; (2) published and distributed freely, without restriction; and (3) available in the form of physical documents such as brochures, formal statements, press releases, reports, web pages, and bulletin boards accessible with anonymous access.

5.1.4.3 The greatest security threat to unrestricted data is

from unauthorized or unintentional alteration, distortion, or destruction. Security controls appropriate to the system containing this data must be in place to maintain its integrity.

5.1.4.4 Examples of unrestricted data may include the following:

5.1.4.4.1 Occupational licensing data excluding social security numbers;

5.1.4.4.2 Agency public websites; and

5.1.4.4.3 Statewide policies.

5.2 Data Criticality

Data and systems should be put into appropriate classification levels according to their criticality. The levels of criticality and their descriptions are as follows:

5.2.1 Level A – **Extremely Critical** – These data and systems are critical to public health or safety and must be protected by a vital plan allowing the continuation of operations within a very short timeframe. These data and systems also require restoration of the original facilities to be able to resume business and might require availability within two hours.

5.2.2 Level B – **Critical** – These data and systems are required in order to administer functions within State government that need to be performed. Business continuity planning allows the State to continue operations in these areas within a certain period of time until the data and systems can be restored and might require availability within eight hours.

5.2.3 Level C - **Not critical** – These data and systems are necessary to State government, but short term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of the citizens of West Virginia.

6.0 ENFORCEMENT

Any agency found to have violated this policy may be subject to an accountability review by Department and/or State leadership. Any action, if determined to be necessary, will be administered by the appropriate authority and may be based on recommendations of the West Virginia Division of Personnel, intended to address severity of the violation and the consistency of sanctions.

7.0 LEGAL AUTHORITY

Under the provisions of West Virginia Code §5A-6-4a *et seq*., the Chief Technology Officer (CTO) is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

This policy is one in a series of Information Technology (IT) related policies intended to define and enable the incorporation of appropriate practices into all activities using State-provided technology in the State of West Virginia.

To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than Information Security policies issued by the WVOT the more restrictive provisions will prevail.

8.0 DEFINITIONS

8.1 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

8.2 Confidential Data – Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.

8.3 Contractor – Anyone who has a contract with the State or one of its entities.

8.4 Criticality - Being of the highest importance. The level at which it data must be protected from non-recovery.

8.5 Data owner – The person having primary responsibility for the creation and maintenance of the data content.

8.6 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

8.7 Sensitivity - The level at which data must be protected from disclosure.

8.8 System – A combination of hardware, software, and procedures necessary to support particular data. A server may have multiple systems and a system may require multiple servers.

8.9 System Owner - The individual who has overall responsibility for a computer application. This person might be required to approve design changes, updates, new reports, system access, or any other action pertaining to the disposition of the application, or data associated with that application. This person would be a subject matter expert (SME) on the system's purpose, hardware requirements, communications requirements, funding requirements, user criteria, etc.

8.10 West Virginia Division of Personnel – The Division of the Department of Administration established by WV Code § 29-6-1 et seq., which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

8.11 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.,*

which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

9.0 INDEX

Attachment A - Data Sensitivity and System Criticality Grid

**** Rows Represent Data Sensitivity** **** Columns Represent System Criticality**	Level A - **Extremely Critical** Critical to health or safety: These systems must be protected by a vital plan that would allow resumption of operations within a very short timeframe. It also requires the ability to be able to resume business.	Level B - **Critical** Required to perform a critical service of State government: These systems will be required in order to administer critical functions within State government. Business continuity planning allows State government to continue operations in these areas within a certain period of time until the system can be restored.	Level C - **Not Critical** Necessary to State government but short-term interruption of service acceptable. These systems do not play any role in the scheme of health, security, safety of the citizens, etc. They could be easily offset with manual procedures.
Level 1 – **Extremely Sensitive** Data whose disclosure or corruption could be hazardous to life or health (ex: State law enforcement records).	**1A**	**1B**	**1C**
Level 2 - **Very Sensitive** Data only available to internal authorized users. May be protected by federal and state regulations. Intended for use only by those who require information in the course of performing job functions (ex: SSNs, credit card #s, home addresses).	**2A**	**2B**	**2C**
Level 3 - **Sensitive** Public Data with limited availability, but which requires a special application to be completed or special processing to be done prior to access (ex: State personnel records, data elements in motor vehicle records not restricted by privacy regulations, etc.).	**3A**	**3B**	**3C**
Level 4 - **Unrestricted** Open public data with no distribution limitations, anonymous access. May be anonymous access via electronic sources.	**4A**	**4B**	**4C**